ABSTRACT OF THE DISCLOSURE

A packet interception system intercepts message packets transmitted from a packet source or to a packet destination, and processes them so as to facilitate verification of the contents and the sequence with which the message packets are intercepted, and for storing the processed message packets for later use. The packet interception system generates for each intercepted message packets respective hash values based on the respective intercepted message packet and the hash value generated for the previously-intercepted message packet, or, for the first intercepted message packet, a value that is provided to identify the session. To verify a previously-stored intercepted message packet, the packet interception system, or another device, using the same hash algorithm, can process the sequence of stored intercepted message packets up to and including the intercepted message packet to be verified, to and compare the hash value generated to the previously-generated hash value for each of the message packets. If the sequence of hash values so generated corresponds to the previously-stored sequence, both the integrity and the sequence of message packets is verified. In addition to the hash values, the packet interception system can, for selected ones of the intercepted message packets, generate digital signatures using any convenient encryption algorithm.